نسرين فوزى اللواتى

الصين.. وأمريكا.. والجيل الخامس..

التنين الصينى وفن إخضاع العدو دون قتال

أثارت القيود التى فرضتها الولايات المتحدة الأمريكية مؤخرا، وألزمت بها بعض الشركات الأمريكية بمقاطعة شركة "هواوى"، والتى كان من أبرزها منع هواوى من استخدام نظام التشغيل أندرويد، وتطبيقاته بسبب ما اعتبرته "مخاوف تتعلق بالأمن القومى الأمريكى" الجدل حول طبيعة الصراع الدائر بين البلدين.. وقد نشرت « لغة العصر» فى عددها رقم 212 الصادر فى أغسطس 2018 تقريرا يتناول المعلومات التى أثيرت بحجم الاستثمارات الضخمة التى سيولدها الجيل الخامس طبقا لتقديرات شركة IHS للأبحاث حيث توقعت أن يصل حجمها إلى حوالى 12.3 تريليون دولار (12 ألف مليار و300 مليار دولار أمريكى). وسنتطرق فى هذا التقرير إلى أبعاد أكثر عمقا تتعلق بحجم الصراع الذى لا يتعلق بالولايات المتحدة والصين فقط، بل تتداخل فى تعقيداته عشرات الدول الأخرى، ولا يشمل شركة "هواوى" فقط، بل يدخل فى نطاقه عدة شركات صينية أخرى.

أشرف شهاب

نشر "مركز التميز للدفاع السيبرانى التابع لمنظمة حلف شمال الأطلنطى" The NATO Cooperative Cyber Defence Centre of Excellence-CCD-COE وهو مركز بحثى للدفاع السيبرانى معتمد من حلف شمال الأطلنطى "الناتو"، يركز على الأبحاث والتدريب فى نهاية شهر مارس الماضى تقريرا تحت عنوان: "هواوى والجيل الخامس والصين كتهديد أمنى" Huawei, 5G and China as a Security Threat. ويشير التقرير إلى أن العقوبات التى فرضتها كل من أمريكا، وأستراليا، ونيوزيلندا، واليابان، وجمهورية التشيك على استخدام حلول الجيل الخامس للاتصالات المحمولة التى تقدمها شركة "هواوى" أثارت حفيظة عدد من المتحمسين لتقنيات الجيل الخامس الذين يعتقدون أن من شأن تلك الإجراءات إبطاء نشر شبكات الجيل الخامس على مستوى العالم.

تتركز المخاوف الحقيقية أو المتصورة لمعظم الدول من شركات التكنولوجيا الصينية بشكل عام، حول طبيعة العلاقات بين تلك الشركات وأجهزة الاستخبارات الصينية، التى يعززها القول بأن البيئة السياسية والقانونية الصينية تفرض على تلك الشركات التعاون مع وكالات الاستخبارات، وبالتالى، الشعور بأن استخدام الحلول التقنية التى تقدمها شركة "هواوى" سيعنى ضمنيا الاعتماد التام على معدات يمكن أن تتحكم فيها أجهزة المخابرات الصينية والجيش سواء فى أوقات السلم أو الحرب.

التنين الصينى يأخذ زمام المبادرة

نجحت شركات التكنولوجيا الصينية على مدى العقود القليلة الماضية فى امتلاك زمام المبادرة التكنولوجية وقيادة العالم تقنيا، بسبب تبنيها لسياسات تعتمد على الإبداع، والابتكار والجودة الفائقة بشكل ملحوظ، بالإضافة إلى انخفاض التكلفة. ويبدو أن هذا التفوق التقنى الصينى قد أثار فزع الغرب من الوقوع تحت هيمنة التنين الصينى الذى لم يخف نيته السعى بنشاط للتفوق، ومن ثم الحصول على نفوذ عالمى أقوى، مما يثير مخاوف مستقبلية بأن ذلك التفوق يحمل فى طياته تهديدات على الأمن القومى والاقتصادى والاجتماعى لتلك الدول يؤدى فى نهاية الأمر إلى زعزعة استقرارها خصوصا، مع شكاواهم الدائمة من أن الصين تعتمد سياسات تجسس سيبرانية، وتنتهك حقوق الملكية الفكرية.

الجيل الخامس ليس مجرد تقنية

فى ظل المخاوف الغربية المتأصلة تاريخيا تجاه الصين، يأتى تملكها لزمام القيادة فى تقنيات الجيل الخامس كعنصر إضافى يزيد الأمور اضطرابا، إذ أن طبيعة وإمكانات الجيل الخامس لا تقتصر على كونه مجرد تقنية جديدة، واعدة، توفر جودة فائقة، وإمكانيات مبتكرة. فشبكات الجيل الخامس تمتلك فى طياتها إمكانية أن تصبح النظام العصبى الرقمى للمجتمعات المعاصرة. ومع عدم وجود ضمانات بأن تكون التكنولوجيا آمنة تماما، والوضع بعين الاعتبار مخاطر حدوث ثغرات أمنية غير متوقعة يمكن استغلالها من قبل جهات معادية. فإن قدرات الصين المعروفة، وميلها للاستفادة من هذه الميزات، يجعل مسألة نشر الجيل الخامس أكثر من مجرد مسألة فنية يمكن النظر إليها على ضوء اعتبارات محددة، لأن الاختيارات التكنولوجية يمكن أن تكون لها آثار أمنية اقتصادية وقومية على حد سواء.

وتعتقد الدول الغربية أنه عند النظر فى الإمكانات الهائلة التى تحملها تقنيات الجيل الخامس، فإنه لا يمكن بأى حال من الأحوال الفصل بين منظور الاستخدامات المدنية أو الدفاعية، إذ أن منظمات الأمن والدفاع الوطنية



تســتخدم إلى حد كبير البنيــة التحتية المدنية، وتمتلــك التفويضات اللازمة للتدخــل لحمايتها أثنــاء الأزمات. وبما أن المزيد مــن التقنيات "الرقمية" أو "الذكية" تجد طريقها إلى العمليات العسكرية، فإن من الصعب التفكير في إنشاء بنية تحتية رقمية موازية منفصلة مخصصة للاستخدامات الدفاعية.

الجيل الخامس والتهديدات الأمنية

يوفــر الجيل الخامس من الاتصالات المحمولة ســرعات أكبر فى نقل البيانات ووقت استجابة أقل (استجابة أفضل) وإمكانية الاتصال فى وقت واحد بملايين الأجهزة "إنترنت الأشــياء". وبالتالى فإن ســرعة تطبيق ونشــر تقنيات الجيل الخامس سوف يسرع من تقدم تقنيات الروبوتات وعمليات الأتمتة، وسيدعم بشكل متقدم تقنيات "الواقع الافتراضى" Virtual Reality-VR و"الواقع المعزز" Augmented Realty-AR، و"الــذكاء الاصطناعــى" Artificial Intelligence-AI والتعلــم الآلــى Macine Learning_ML. وهو ما يعنى أننا أمام تقنية ســتقوم بتغيير المشهد العالمى للأجهزة والتطبيقات بشكل جذرى، وستقوم بتحويل المجتمعات إلى مجتمعات رقمية بالكامل، وهى تحولات يصعب تخيلها اليوم.

وفى إطار التكهنات القائمة ولكنها ليست واقعية أو مدعومة بأدلة ملموسة، تعتقــد أمريكا وحليفاتهــا من الدول الغربية أن قيــام الجيل الخامس بربط مليــارات الأجهزة بالشــبكات يعنى زيادة هائلة فى الأهــداف المحتملة وفى وســائل التجسس، ناهيك عن إمكانية اســتخدامها كمنصات استخبارات عن طريق التقاط الإشارات الناشئة عنها لتمكين جمع وتحليل بيانات القياس عن بعد على نطاق واسع.

كما تقلل تقنية الجيل الخامس من الفصل بين شــبكات الاتصالات الطرفية والشــبكات الأساســية، مما يعنى أنه الصعب الحد مــن تأثير البائعين ليس فقط على الشــبكات الأساســية بل على الشــبكات الطرفية ايضا، مما يعنى أن أى تهديد محتمل للشــبكة ســيكون تهديدا شــاملا لكامل الشبكة، وفى هذه الحالة سيكون من الصعب، بل ربما من المستحيل التراجع عن استخدام الشــبكات التى تم تركيبها، لأن أى محاولة لتغيير التقنية المعتمدة سيكون معناها الإضطرار إلى تغيير هيكلية الشبكة بالكامل، وهو أمر معقد، ومكلف، ويستغرق وقتا طويلا.

لماذا هواوى؟

يشــير التقرير الذى أشــرنا إليــه إلى أن صعود نجم شــركة "هــواوى" على المستوى العالمى يعتبر مثالا حيا على السياسات التى اتبعتها الصين للتفوق التكنولوجــى، وريادة العالم فى هذا المجال. فقد شــهدت الســنوات القليلة الماضيــة نمو الشــركة لتصبح أكبر شــركة لتصنيع معــدات الاتصالات على مســتوى العالم. وفى عام 2018 تفوقت "هواوى" على شركة "أبل" لتصبح ثانى أكبر منتج للهواتف الذكية بعد شــركة "سامســونج" الكورية الجنوبية. وتعد شركة "هواوى" حاليا الشركة الوحيدة التى يمكنها إنتاج جميع عناصر شــبكة الجيل الخامس، على نطاق واســع وبتكلفة معقولة، والأهم من ذلك بلا منافســة حقيقية، إذ أن أقرب منافســيها "نوكيا" و "إريكســون" ما زالا غير قادرين حتى اللحظة على تقديم بديل قابل للتطبيق، مما أفسح المجال واســعا أمام هواوى للسيطرة على سوق الاتصالات اللاسلكية للجيل الخامس تقريبــا، وأتاح لهــا أن تتعاون مع كبريات شــركات الاتصــالات فى عدد من البلدان الأوروبية، وفى جميع أنحاء العالم.

براءات الاختراع كعنصر تفوق

يرجــع الفضل فى تفوق "هــواوى" وغيرها من شــركات الاتصالات الصينية الأخــرى فــى تقنيات الجيل الخامس إلــى تاريخ طويل من الإبــداع والابتكار، والتطوير، حيث تمتلك الشــركات الصينية نســبة كبيرة من بــراءات الاختراع الأساســية للجيــل الخامــس. وتمتلك الصين حاليــا ما يقرب مــن 10 ٪ من حقوق الملكية الأساسية لتقنيات الجيل الخامس. وتأتى "هواوى" على رأس الشــركات فى نســب براءة الاختراع، تليها شــركة ZTE. بالإضافة إلى النفوذ

> فن الحرب الأسمى
> هو إخضاع العدو دون قتال
>
> **صن تزو**
> الجنرال الصينى والاستراتيجى العسكرى والكاتب والفيلسوف

الصينــى المتصاعد فى المنظمات الدولية المعنيــة بوضع معايير الاتصالات العالمية، كالاتحاد الدولى للاتصالات ITU، ومشــروع شراكة الجيل الثالث 3G Partnership Project.

اقتصاديات الحجم

يعد حجم السوق الصينى الأضخم فى العالم من حيث عدد السكان 1.42 مليار نســمة (مليار و420 مليون نســمة)، من العوامل المؤثرة فى نمو الشــركات الصينية بشــكل كبير، بالإضافة إلى السياسات التى تتبعها الحكومة الصينية لتشجيع الشــركات، حيث أعلنت الحكومة الصينية مرارا عزمها أن تصبح قوة عظمــى فــى التكنولوجيا الرقمية. ووضعــت عام 2006 اســتراتيجية طويلة الأجــل للابتكار كان من بين أهدافها الابتكار التكنولوجى، وفك الارتباط عن الغرب. وتــم دعم هذا الجهد مــن بتركيز الاســتثمارات الحكومية فى مجال البحث والتطوير التكنولوجى. ومن خلال تقييد وصول الشــركات الغربية إلى الســوق الصينية، تمكنت الصناعة الصينية من الاســتفادة من حجم الســوق المحلية، دون منافسة أجنبية (تسيطر الشركات الصينية على 75 ٪ من السوق الصينى). ومع النجاح الذى لقيته الاســتراتيجية الوطنية الصينية، تم تعزيزها باســتحواذ رأس المال الصينى على العديد من شــركات التكنولوجيا والبنية التحتية الأمريكية والغربية.

أنشطة هواوى

لا يوجــد حتى هذه اللحظة أى دليل، علــى الأقل علنا، على وجود نقاط ضعف كبيرة فى التقنيات التى تقدمها شركة "هواوى" ولا توجد أى أدلة ملموسة على تورطها فى أعمال تجســس. ومع ذلك، فقد تم إلقاء اللوم على الشركة مرارا وتكرارا بســبب التجسس الصناعى (قضية Cisco عام 2003 وقضية T-Mobile عام 2014). وحتى المزاعم بأن الحكومة الصينية تنتهك العقوبات الاقتصادية الدولية ضد إيران وكوريا الشــمالية، لا علاقة قوية بينها وبين الاتهامات الموجهة لشــركة "هــواوى". ومع ذلــك، تم توجيــه الاتهامات لشركة "هواوى" بالتجســس، وربطت تقارير خاصة بالاستخبارات الأسترالية العام الماضى بين موظفى "هواوى" وعمليات تجسس عن طريق الحصــول على رمــوز دخول والتســلل إلى شــبكات محلية. كما احتجزت كل من كندا وبولندا فى الأشهر الأخيرة اثنين من مسئولى شركة "هواوى"، بينهما ابنة مؤسس ورئيس شــركة "هواوى". ونفت شركة "هواوى" عدة مرات على لسان عشرات المسئولين من أبرزهم مؤسس الشركة ورئيسها "رن تزنفيه"، الذى أكد مرارا وتكرارا أن أسهم الشركة مملوكة من قبل موظفين، وأنها ليست ملكا لأى حكومة، وأنها لم تستخدم معداتها للتجسس أو التخريب فى بلدان أخرى. كما نفى بشكل قاطع أن تكون "هواوى" قد قدمت أو قامت فى أى وقــت مضى بتقديم معلومات عن العملاء لأى حكومة أو مؤسســة".



رن تزنفيه
مؤسس ورئيس شركة هواوى

وإثباتا لحســن نيتها قامت "هواوى" بإنشاء عدة مراكز لتقييم الأمان Huawei Cyber Security Evaluation Centre-HCSEC الخــاص بمنتجاتها فى المملكة المتحدة، وألمانيا، ومؤخرا فى العاصمة البلجيكية بروكســل لتزويد الشــركاء بفرصة لتقييم منتجات الشــركة عن كثب والتأكد من عدم وجود أى أنشــطة مشــبوهة، بل، وأتاحــت لهم "الكود المصدري" لمنتجاتهــا للمزيد من إثبات حســن النية. وتؤكد الشركة دائما فى بياناتها أنها: "شركة التكنولوجيا الأكثر تدقيقا فى العالم". ويعتبر "مركز التقييم" الذى أنشــأته شركة "هواوى"فى المملكة المتحدة HCSEC من خلال مجلسه الرقابى الذى تسيطر عليه "هيئة الأمن الســيبرانى" National Cyber Security Centre-NCSC والذى يتبع Government Communications Headquarters (GCHQ وهــى وكالة تابعة لجهاز الاســتخبارات والأمن البريطانية، فريدا حتــى الآن فى نموذج عمله. لدرجة أن المراكز المماثلة التى أشرنا إلى إنشائها فى ألمانيا وبلجيكا تفتقر إلى إشراف مماثل.

وعلى الرغــم من كل تلك الضمانات التى قدمتها "هواوى" إلا أن الحكومات الأوروبيــة تعتقد أنه حتى فى حالة عدم وجود علاقة رســمية بين شــركات التكنولوجيا الصينية والحكومة الصينية، فإن البيئة القانونية الصينية مواتية وتسمح للحكومة الصينية باستخدام الشركات الخاصة وتكنولوجياتها كأدوات للتجسس.

ليست هواوى فقط

كما يشير تقرير CCDCOE إلى أنه على الرغم من التركيز الشديد على شركة "هــواوى" كمتهم، بســبب قدراتهــا المتطورة فى تقنيــات الجيل الخامس،



إلا أن القضيــة لا تتعلق بشــركة "هواوى" فقط. فالعديد من الدول تشــعر بالقلق أيضا بشأن العديد من الشركات الصينية الأخرى المصنعة لتكنولوجيا الاتصالات، ومن أهم تلك الشــركات شــركة ZTE وهى واحدة من الشــركات الرائدة فى تصنيع معدات الاتصالات فى الصين، وإحدى الشركات الرائدة فى مجال توفير معدات الشــبكات. وتشــمل قائمة منتجاتها الرئيسية الشبكات الأساسية، وشبكات النقل، وشــبكات الوصول اللاسلكى، والثابت، والحوسبة السحابية، وحلول الطاقة. وفى عام 2017 تم اتهام ZTE بتصدير التكنولوجيا الأمريكية بشكل غير قانونى إلى إيران وكوريا الشمالية فى انتهاك للعقوبات الاقتصادية. وفى أبريل 2018، فرضــت وزارة التجارة الأمريكية حظر تصدير لمدة 7 سنوات على منتجات ZTE إلى الولايات المتحدة. وتم رفع ذلك الحظر فــى يوليو 2018 بعد قيــام ZTE بحل مجلــس الإدارة، وموافقتها على دفع غرامات إضافية وإنشــاء فريــق امتثال داخلى للعقوبــات الدولية على إيران وكوريا الشــمالية. وبالإضافة إلى "هواوى" و ZTE تشــمل قائمة الشــركات الصينيــة الأخــرى شــركات مثــل: Hytera Communications Corporation و Hangzhou Hikvision و Dahua Technology

وتعد شــركة Hytera ثانى أكبر شركة مصنعة لمحطات توزيع الطيف الترددى عالميا حيث تمتلك 13 ٪ من حصة السوق العالمى. وهى تنتج أنظمة DMR و LTE و MPT-1327 بالإضافــة إلى أنظمة TETRA التى تم تصميمها خصيصا للاســتخدام من قبل الوكالات الحكومية، وخدمات الطوارئ وشبكات السلامة العامة وخدمات النقل (السكك الحديدية على وجه الخصوص) والاستخدامات العسكرية. أما شركتا Hikvision و Dahua Technology فهما المزودان الصينيان لمنتجات المراقبة بالفيديو، وهما يحتلان المركز الأول والثانى من حيث الحصة الســوقية على مستوى العالم. وجميع هذه الشركات الثلاث تم حظر استخدام تكنولوجياتها فى الشبكات الحكومية بموجب القانون الأمريكى.

التجسس والتأثير

يشــير تقرير CCDCOE إلى أن المخاوف الأمنية الغربية الأمريكية والأوروبية بشــأن استخدام التكنولوجيا الصينية قديمة، وتزايدت مع بزوغ نجم الصين، وتصاعــد موقعهــا فــى الأســواق العالميــة. كان المســئولون الحكوميون الغربيون والمجتمع الأمنى قلقين بشــأن إمكانية استخدام الحكومة الصينية والجيش الصينى للتكنولوجيا التى تنتجها الشــركات الصينية للتجسس على المســتخدمين، بسبب ما أسماه التقرير تمتع الصين بسمعة سيئة فى مجال التجسس الصناعى، وكذلك التعاون الوثيق بين الحكومة والصناعة الصينية فى "استهداف المؤسسات الأكاديمية والصناعة والمرافق الحكومية لغرض جمع الأسرار التكنولوجية".

وهنــاك مجموعة طويلة من الأمثلة التــى يتم التدليل بها على تلك المزاعم باســتخدام القدرات الســيبرانية الحكومية والعســكرية لأغراض التجســس الاقتصادى. ففى عام 2013، أصدرت شــركة Mandiant (شركة أمن سيبرانى أمريكيــة) تقريرا أشــارت فيه إلــى حملة تهديد متواصل لســنوات متعددة، ربطت فيه بين مجموعة تســمى: APT-1 وجيش التحرير الشــعبى الصينى. وقامت باستعراض ما قالت إنه قيام تلك المجموعة بسرقة منهجية لبيانات سرية من أكثر من 140 منظمة تعمل فى صناعات متعددة.

وفى شــهر ديســمبر الماضى 2018، أعلنت المملكة المتحــدة وحلفاؤها أن مجموعة معروفة باســم APT-10 تعمل نيابة عن وزارة أمن الدولة الصينية للقيام بحملة سيبرانية ضارة تســتهدف الملكية الفكرية والبيانات التجارية الحساسة فى أوروبا وآسيا والولايات المتحدة الأمريكية.

أمــا فــى الولايات المتحــدة الأمريكيــة، فمن بيــن جميع قضايا التجســس الاقتصــادى التــى نظرت فيهــا وزارة العدل بين عامــى 2011 و 2018 كانت الصين عنصرا مشتركا بنسبة 90 ٪.

البيئة القانونية والسياسية فى الصين

يشــير تقرير CCDCOE إلى أن قانون الاســتخبارات الوطنى الصينى الصادر عام 2016 يشترط على جميع الشركات، دعم وتقديم المساعدة والتعاون فى عمل الاستخبارات الوطنية، وضمان سرية أى عمل استخبارى وطنى يحيطون بــه علما. وتحمى الدولة الأفراد والمنظمات التى تدعم وتعاون وتتعاون فى عمــل الاســتخبارات الوطنية. وعلى نفــس المنوال، يفــرض قانون مكافحة التجسس الصينى لعام 2014 التزامات على "المنظمات والأفراد ذوى الصلة" تقديم المعلومات أو التسهيلات أو غيرها من المساعدات، ويؤكد للمنظمات والأفــراد المعنيين بأنه "يجب ألا يرفضوا" التعــاون. وهذه المواد القانونية تثير مخاوف عميقة فيما يتعلق بوضع الشركات الصينية فى حالة رأت الدولة الصينيــة أن ذلك التعاون ضرورى طبقا لمفهومها المتمثل فى الحفاظ على أمن الدولة الصينية.

الصين والحقوق الفردية

تختلــف المقاربات الصينية والغربيــة تجاه الحقوق الفرديــة اختلافا جذريا. فعلــى ســبيل المثال يتخــذ الاتحــاد الأوروبى موقفــا صارما بشــأن حماية الخصوصيــة الفرديــة، كما يتضح من خــلال تطبيق اللائحــة العامة لحماية البيانات (GDPR) ما قد يعنى تفضيل الحقوق الخاصة على حقوق الدولة. فى حين يسود الاعتقاد بأن الصين تعمل بمنهج مختلف يفضل مصلحة الدولة علــى المصالح الخاصة، ومن هنا ينشــأ تخوف آخر يقــول إنه على الرغم من أن شركات مثل "هواوى" تخضع للقوانين المحلية للبلدان التى تعمل فيها، إلا أن المصالح المتداخلة والمتشــابكة للشركة يمكن أن تضعها فى منطقة اختصاصات قضائية متشابكة قد تجبر الشركات الصينية فى نهاية المطاف على التعاون مع وكالات الاستخبارات الصينية.

ويدعــم هذه المخاوف تقرير التحقيق الذى أجرته لجنة الاســتخبارات بمجلس النواب الأمريكى فى عام 2012 حيث توصل التقرير إلى ما مفاده فشل شركة "هواوى" فى "الكشف عن تفاصيل تعاملاتها مع الجيش أو أجهزة المخابرات الصينية" ورفضها "تقديم إجابات واضحة عن آليات صنع القرار داخل الشركة". كمــا قال التقرير إن اللجنة لم تتلق أى معلومــات تقريبا عن دور لجنة الحزب الشيوعى الصينى فى شركة "هواوى" أو تعاونها مع الحكومة الصينية.

قيود القانون الدولي

نظرا لأن الخطر الرئيسى المتمثل فى استخدام التكنولوجيا الصينية ينبع من التأثير الذى يمكن أن تمارسه الحكومة الصينية على الشركات الصينية. ومع الإقرار بأن سلطة الصين السيادية على شئونها الداخلية تعنى أنها حرة فى فــرض التزامات على صناعاتها، بما فى ذلك لغرض التعاون الاســتخباراتي. فإن الجانب الآخر من ممارســة حقوق السيادة، يعنى أيضا أن الدول الغربية حــرة من حيث المبدأ فــى حظر المنتجات الصينية، بشــرط احترام التزاماتها الناشــئة بموجب ترتيبــات التجارة الدولية، خاصــة الاتفاقية العامة لمنظمة التجــارة العالمية بشــأن التعريفات الجمركية والتجــارة (GATT) التى تغطى التجارة الدولية فى البضائع.

وبما أن شبكات الاتصالات الأساسية بنية تحتية أساسية، وبالتالى فهى مصلحة وطنية أساســية، لها آثار على الأمن القومــي. وبالتالى فإن اعتماد تكنولوجيا "هواوى" أو ZTE أو أى شــركة صينية أخرى كشــبكات اتصالات أساسية يعنى أنها ستصبح جزءا من البنية التحتية الأساسية للاتصالات فى عشرات البلدان. وهذه البنية التحتية سيتم الاعتماد عليها لأداء مجموعة من الخدمات الأساسية، والوظائف الاجتماعية والاقتصادية. وهذا يعنى أن نشــر تكنولوجيا "هواوى" سيجعلها تتغلغل فى مكونات مهمة فى الأنظمة ذات الأهمية الاستراتيجية للمجتمعات، بما فى ذلك الخدمات الأمنية والعسكرية، خصوصا إذا تطلب الأمر الاعتماد على تلك التكنولوجيا ولو بشكل جزئى أثناء الأزمات.

التبعية الرقمية

إن أهمية البنية التحتية الأساسية لعمل المجتمع تجعل من نشر البنية التحتية للاتصالات قرارا اســتراتيجيا ليس فقط لمشــغلى الاتصالات، ولكن بالنسبة للأمــة بأكملها، خاصة وأن من المتوقع أن تؤدى تقنيات الجيل الخامس إلى نمو هائل فى الخدمات التى تدعم إنترنت الأشــياء (ليس فقط درجة التبعية الرقمية للمجتمعــات المعاصرة بل طابعها ذاته). لذلــك، قد يكون للحادث

الســيبرانى المحتمل درجات مختلفة من التأثير على الأمن القومي والمصالح الوطنية الحيوية. وبما أنه من الصعب اســتبعاد أى من هذه المخاطر بشكل أساســى، فإن موثوقية الشــركات الموردة للشبكات كشــريك لمنع وكشف الثغــرات المحتملة، والتعاون فى تخفيف المخاطر تنطوى على أهمية بالغة. ونظــرا لتكلفــة وصعوبة اســتبدال أو تكرار إنشــاء مثل هــذه البنية التحتية الأساســية، تعتقد الــدول الأوروبية أن عليها موازنــة المخاطر المحتملة من الشــركات الموردة للبنية التحتية بشكل شــامل، ومسبقا. وعلاوة على ذلك، ونظرا لديمومیتها النســبية، يمكن أن يكون لقرارات نشر البنية التحتية آثار طويلــة المدى على التعاون مع الشــركاء الدوليين والحلفاء بســبب المخاطر المحتملة على مشــاركة المعلومات الحساســة ، وهو ما حذرت منه الولايات المتحدة حلفاءها فى حلف "الناتو" مؤخرا.

علــى ضــوء هذه المخــاوف، اختــارت عدة دول فــرض قيود على اســتخدام التكنولوجيا الصينية فى بنيتها التحتية الأساسية. بعض الدول اختارت إصدار توجيهــات ملزمة لقبول أو تقييد التكنولوجيا الصينية كما فى حالة الولايات المتحدة وجمهورية التشيك، وأستراليا، واليابان التى أصدرت إرشادات أمنية إلزامية تســتثنى نشــر معدات البنية الأساســية من مقدمى الخدمات الذين يحتمل أن تســيطر عليهم حكومات أجنبية. وفــى المقابل تدخلت نيوزيلندا بقوة وأجبرت شــركات الاتصالات على عدم اعتمــاد تقنيات "هواوى" للجيل الخامس على أســاس قانون الاتصالات لعــام 2013 (بموجب حق الاعتراض) بسبب "مخاطر الأمن القومى".

وتبنت الولايات المتحدة قانونا فى عام 2018 يحظر شراء واستخدام منتجات الاتصــالات والمراقبة الموردة من شــركات صينية محددة. وتحدت "هواوى" مؤخرا هذه الخطوة باعتبارها: "غير دستورية"، و "مقيدة للمنافسة العادلة"، ومضرة للمســتهلكين الأمريكييــن، لكن من المتوقع عــدم قبول اعتراض "هواوى".

حبر على ورق

فــى المقابل اختــارت بعض الدول الامتناع عن فرض قيــود على "هواوى". فقد أشار رئيس المكتب الفيدرالى الألمانى لأمن المعلومات (BSI) فى أكتوبر 2018 إلــى أن هناك حاجة إلى أدلــة واضحة وجادة من أجل فرض حظر على معدات "هــواوى". ومــع ذلك، تغيــر موقف ألمانيــا. وفــى فبراير الماضــى 2019 ألمحت التقارير الصحفية إلى أن ألمانيا تطالب بعقد اتفاقيــة "عدم تجســس" مماثلــة للاتفاقية التــى عقدتهــا الولايات المتحــدة مع الصين عام 2015 (تزعم الولايات المتحدة أن الصين تخلت عن الاتفاقية فأصبحت حبرا على ورق). وفى ســلوفاكيا قال رئيس الوزراء إن بلاده لا تعتبر "هواوى" تهديدا أمنيا، وأنها بحاجة إلى دليل قبل فــرض أى قيــود. ونفس الموقف عبر عنــه عبد الله بــن عامر الســواحة، وزير الاتصالات وتقنية المعلومات السعودى الذى صرح مؤخرا أن بلاده لا تعتبر أن "هواوى" تشكل تهديدا أمنيا.


عبد الله بن عامر السواحة
وزير الاتصالات
وتقنية المعلومات السعودي

مخاطر محتملة ولكن

حتى فــى حالة وجود تخوفات من "هواوى" وغيرها من الشــركات الصينية، فإن بإمكان العديد من الدول اللجوء إلى وسائل محددة أو مخصصة للتخفيف مــن المخاطر، خصوصــا مع إعلان "هواوى" الدائم اســتعدادها ورغبتها فى التعــاون. ومن أمثلة ذلــك التعاون كما أشــرنا مراكز الأمن الســيبرانى فى المملكة المتحدة وألمانيا وبلجيكا، الذى تم إنشاؤه عام 2010 لتقييم أجهزة وبرامــج "هــواوى"، ويخضع لرقابة هيئة الأمن الســيبرانى التى هى جزء من وكالة الاســتخبارات والأمن البريطانيــة، حيث يتم إصدار تقارير منتظمة عن النتائــج التى يتم التوصل إليهــا، وآخرها فى يوليــو 2018 وقد أدرك رئيس هيئــة الأمن الســيبرانى مؤخرا أن هذه الرقابة الرســمية المفصلة، تعنى أن نظــام المملكة المتحدة هو نظام الرقابة الأشــد والأكثــر صرامة فى العالم علــى "هــواوى"، وأنه يثبت جــدواه يوما بعد يوم. نفــس الأمر ينطبق على المركــز الــذى أقامته "هواوى" فــى ألمانيا فى نوفمبــر 2018 " للتعاون مع العملاء والشركاء والمؤسسات البحثية الألمانية، وكذلك السلطات الحكومية والإشــرافية"، وينطبق كذلك على "مركز الشفافية الأمنية السيبرانية" التابع للاتحاد الأوروبى فى بروكســل الذى أنشأته "هواوى" فى مارس 2019. وقد عرضت "هواوى" إنشاء مركز مماثل فى بولندا.

حلول بديلة وتفاعلات دولية

يعد تســريع نضوج مقدمــى الخدمات البديلــة أحد الخيارات. فعلى ســبيل المثال أبدت "كندا" منتصف يناير 2018، اهتمامها بالحلول البديلة المنافسة لتقنيات "هواوى" ونظرت بعين الاعتبار إلى التكنولوجيا التى تقدمها شركة "نوكيا" من خلال قيامها بمنح الشركة 40 مليون دولار لتمويل عمليات البحث والتطوير المتعلق بتقنيات الجيل الخامس. ويعتقد الخبراء فى CCDCOE أن مثل هذه الوسائل سوف تساعد على تحفيز تنوع العروض فى السوق العالمى لمنع الهيمنة غير المرغوب فيها على الســوق من شركة واحدة، بغض النظر عن المنشأ، أو أى مخاطر أمنية محتملة.

وفــى ديســمبر 2018 أعلنــت مجموعــة الاتصــالات البريطانيــة BT Group المشــغل لخدمات للاتصالات فى المملكة المتحدة عــن قرارها بالتخلى عن أجهزة "هواوى" لكل من الجيل الثالث والجيل الرابع الحالية، والجيل الخامس المســتقبلية. وذكرت شركة الاتصالات الألمانية دويتشه تيليكوم أنها تراجع إســتراتيجياتها تجاه مــزودى الأجهــزة والمعــدات. وأعلنت شــركة "اورنج" الفرنسية أنها لن تستخدم أجهزة "هواوى". وأعلنت شركة TCD، أكبر مشغل للاتصالات فــى الدنمارك، أنها اختارت شــركة "إريكســون"كمورد لمعدات الجيل الخامس، ولكنها بررت قرارها بأنه بسبب"اعتبارات الجودة".

ليست مسألة تقنية فقط

لا يوجــد حتى الآن أى دليل عام على وجود ثغــرات تقنية خطيرة فى أجهزة "هواوى" أو ZTE ومع ذلك، من المســتحيل بشــكل أساســى استبعاد عيوب التكنولوجيــا المحتملة التى يمكن اســتغلالها فى المســتقبل. ســواء كانت هذه التكنولوجيا صينية أو غير صينية، وســواء كانــت الثغرات الأمنية نتيجة لإجراء متعمد أو قابلة للاستغلال بسبب الفشل فى تصحيح البرامج أو عيوب التصنيع، أو عيوب الاستخدام السىء من جانب المستخدمين.

ســيظل هذا الأمر مصدر قلق لأن شــراء تقنية معينة من شركة معين يخلق درجة من الاعتماد على هذا البائع، لأن شراء التكنولوجيا الرقمية لا يقتصر على شراء "المعدات"، بل ينطوى أيضا على التزام طويل الأمد بعلاقة استراتيجية مع الشــركة الموردة للمعدات. وبالنظر إلى هذه الاعتبارات المسبقة، يمكن القول إن جوهر مشكلة "هواوى" هو هل يمكن الوثوق فيها؟ وما هى الآليات التــى تعتمد عليهــا هذه الثقة: هل هى مصداقية الشــركة أو انفتاحها على عمليات التحقق أو المساءلة أو أى شيء آخر؟

هل يستطيع الغرب تحمل النتائج؟

وبكل تأكيد لا توجد ردود ســهلة على هذه الأســئلة. ومن المتوقع أن يأتى قرار إغلاق باب التعاون مع "هواوى" والصين بنتائج عكســية، لأنه ســيحرم أوروبا وكثيرًا من الدول حول العالم من فرصة تطوير خدمات الجيل الخامس. وفى نفس الوقت فإن إنعكاسات مثل هذه القرارات على الصين قد لا تكون خطيرة بالحجم المتوقع لأن الشركات الصينية، يمكنها تحمل تبعات مثل هذه القرارات بسبب ما أوضحناه مسبقا عن نطاق وحجم القوة الشرائية المتزايدة للســوق المحلية الصينية، فضلا عن انفتاح الصين ومشــاركاتها النشطة مع عشرات البلدان النامية كأسواق مستقبلية فى إطار مبادرة "الحزام والطريق"، التى تســعى الصين مــن خلالها لمزيد مــن خطط التعاون الواســعة ليس فقط فى قطاعات الاتصالات والتكنولوجيا، بل، وفى تطوير شــبكات الطرق، والسكك الحديدية، والجسور، والطيران المدنى، والموانئ، والطاقة.

كما أن الغرب بإحجامه عن حلول "هواوى" لا يجد على أرض الواقع الملموس بدائل مكافئة لتكنولوجيا "هواوى". والدول الغربية لن تســتطيع فى الغالب تحمل نتائج ما يمكن أن تسببه أزمة "هواوى" من ركود تكنولوجي، خصوصا مع الفوائد الاجتماعية والاقتصادية المتوقعة من الجيل الخامس.